

107TH CONGRESS
1ST SESSION

H. R. 1259

To amend the National Institute of Standards and Technology Act to enhance the ability of the National Institute of Standards and Technology to improve computer security, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

MARCH 28, 2001

Mrs. MORELLA (for herself, Mr. GORDON, Mr. BOEHLERT, Mr. BARCIA, Mr. EHLERS, Mr. ETHERIDGE, and Mr. GUTKNECHT) introduced the following bill; which was referred to the Committee on Science

A BILL

To amend the National Institute of Standards and Technology Act to enhance the ability of the National Institute of Standards and Technology to improve computer security, and for other purposes.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Computer Security
5 Enhancement Act of 2001”.

6 **SEC. 2. FINDINGS AND PURPOSES.**

7 (a) FINDINGS.—The Congress finds the following:

1 (1) The National Institute of Standards and
2 Technology has responsibility for developing stand-
3 ards and guidelines needed to ensure the cost-effec-
4 tive security and privacy of sensitive information in
5 Federal computer systems.

6 (2) The Federal Government has an important
7 role in ensuring the protection of sensitive, but un-
8 classified, information controlled by Federal agen-
9 cies.

10 (3) Technology that is based on the application
11 of cryptography exists and can be readily provided
12 by private sector companies to ensure the confiden-
13 tiality, authenticity, and integrity of information
14 associated with public and private activities.

15 (4) The development and use of encryption
16 technologies by industry should be driven by market
17 forces rather than by Government imposed require-
18 ments.

19 (b) PURPOSES.—The purposes of this Act are to—

20 (1) reinforce the role of the National Institute
21 of Standards and Technology in ensuring the secu-
22 rity of unclassified information in Federal computer
23 systems; and

1 (2) promote technology solutions based on pri-
2 vate sector offerings to protect the security of Fed-
3 eral computer systems.

4 **SEC. 3. SECURITY OF FEDERAL COMPUTERS AND NET-**
5 **WORKS.**

6 Section 20(b) of the National Institute of Standards
7 and Technology Act (15 U.S.C. 278g–3(b)) is amended—

8 (1) by redesignating paragraphs (4) and (5) as
9 paragraphs (7) and (8), respectively; and

10 (2) by inserting after paragraph (3) the fol-
11 lowing new paragraphs:

12 “(4) except for national security systems, as de-
13 fined in section 5142 of Public Law 104-106 (40
14 U.S.C. 1452), to provide guidance and assistance to
15 Federal agencies for protecting the security and pri-
16 vacy of sensitive information in interconnected Fed-
17 eral computer systems, including identification of
18 significant risks thereto;

19 “(5) to promote compliance by Federal agencies
20 with existing Federal computer information security
21 and privacy guidelines;

22 “(6) in consultation with appropriate Federal
23 agencies, assist Federal response efforts related to
24 unauthorized access to Federal computer systems;”.

1 **SEC. 4. COMPUTER SECURITY IMPLEMENTATION.**

2 Section 20 of the National Institute of Standards and
3 Technology Act (15 U.S.C. 278g–3) is further amended—

4 (1) by redesignating subsections (c) and (d) as
5 subsections (e) and (f), respectively; and

6 (2) by inserting after subsection (b) the fol-
7 lowing new subsection:

8 “(c)(1) In carrying out subsection (a)(2) and (3), the
9 Institute shall—

10 “(A) emphasize the development of technology-
11 neutral policy guidelines for computer security and
12 electronic authentication practices by the Federal
13 agencies;

14 “(B) promote the use of commercially available
15 products, which appear on the list required by para-
16 graph (2), to provide for the security and privacy of
17 sensitive information in Federal computer systems;

18 “(C) develop qualitative and quantitative meas-
19 ures appropriate for assessing the quality and effec-
20 tiveness of information security and privacy pro-
21 grams at Federal agencies;

22 “(D) perform evaluations and tests at Federal
23 agencies to assess existing information security and
24 privacy programs;

1 “(E) promote development of accreditation pro-
2 cedures for Federal agencies based on the measures
3 developed under subparagraph (C);

4 “(F) if requested, consult with and provide as-
5 sistance to Federal agencies regarding the selection
6 by agencies of security technologies and products
7 and the implementation of security practices; and

8 “(G)(i) develop uniform testing procedures suit-
9 able for determining the conformance of commer-
10 cially available security products to the guidelines
11 and standards developed under subsection (a)(2) and
12 (3);

13 “(ii) establish procedures for certification of
14 private sector laboratories to perform the tests and
15 evaluations of commercially available security prod-
16 ucts developed in accordance with clause (i); and

17 “(iii) promote the testing of commercially avail-
18 able security products for their conformance with
19 guidelines and standards developed under subsection
20 (a)(2) and (3).

21 “(2) The Institute shall maintain and make available
22 to Federal agencies and to the public a list of commercially
23 available security products that have been tested by pri-
24 vate sector laboratories certified in accordance with proce-
25 dures established under paragraph (1)(G)(ii), and that

1 have been found to be in conformance with the guidelines
2 and standards developed under subsection (a)(2) and (3).

3 “(3) The Institute shall annually transmit to the
4 Congress, in an unclassified format, a report containing—

5 “(A) the findings of the evaluations and tests of
6 Federal computer systems conducted under this sec-
7 tion during the 12 months preceding the date of the
8 report, including the frequency of the use of com-
9 mercially available security products included on the
10 list required by paragraph (2);

11 “(B) the planned evaluations and tests under
12 this section for the 12 months following the date of
13 the report; and

14 “(C) any recommendations by the Institute to
15 Federal agencies resulting from the findings de-
16 scribed in subparagraph (A), and the response by
17 the agencies to those recommendations.”.

18 **SEC. 5. COMPUTER SECURITY REVIEW, PUBLIC MEETINGS,**
19 **AND INFORMATION.**

20 Section 20 of the National Institute of Standards and
21 Technology Act (15 U.S.C. 278g–3), as amended by this
22 Act, is further amended by inserting after subsection (c),
23 as added by section 4 of this Act, the following new sub-
24 section:

1 “(d)(1) The Institute shall solicit the recommenda-
2 tions of the Computer System Security and Privacy Advi-
3 sory Board, established by section 21, regarding standards
4 and guidelines that are being considered for submittal to
5 the Secretary in accordance with subsection (a)(4). The
6 recommendations of the Board shall accompany standards
7 and guidelines submitted to the Secretary.

8 “(2) There are authorized to be appropriated to the
9 Secretary \$1,030,000 for fiscal year 2002 and \$1,060,000
10 for fiscal year 2003 to enable the Computer System Secu-
11 rity and Privacy Advisory Board, established by section
12 21, to identify emerging issues related to computer secu-
13 rity, privacy, and cryptography and to convene public
14 meetings on those subjects, receive presentations, and
15 publish reports, digests, and summaries for public dis-
16 tribution on those subjects.”.

17 **SEC. 6. LIMITATION ON PARTICIPATION IN REQUIRING**
18 **ENCRYPTION AND ELECTRONIC AUTHEN-**
19 **TICATION STANDARDS.**

20 Section 20 of the National Institute of Standards and
21 Technology Act (15 U.S.C. 278g–3), as amended by this
22 Act, is further amended by adding at the end the following
23 new subsection:

24 “(g) The Institute shall not promulgate, enforce, or
25 otherwise adopt standards or policies for the Federal es-

1 tablishment of encryption and electronic authentication
2 standards required for use in computer systems other than
3 Federal Government computer systems.”.

4 **SEC. 7. MISCELLANEOUS AMENDMENTS.**

5 Section 20 of the National Institute of Standards and
6 Technology Act (15 U.S.C. 278g–3), as amended by this
7 Act, is further amended—

8 (1) in subsection (b)(8), as so redesignated by
9 section 3(1) of this Act, by inserting “to the extent
10 that such coordination will improve computer secu-
11 rity and to the extent necessary for improving such
12 security for Federal computer systems” after “Man-
13 agement and Budget)”;

14 (2) in subsection (e), as so redesignated by sec-
15 tion 4(1) of this Act, by striking “shall draw upon”
16 and inserting in lieu thereof “may draw upon”;

17 (3) in subsection (e)(2), as so redesignated by
18 section 4(1) of this Act, by striking “(b)(5)” and in-
19 serting in lieu thereof “(b)(7)”;

20 (4) in subsection (f)(1)(B)(i), as so redesign-
21 ated by section 4(1) of this Act, by inserting “and
22 computer networks” after “computers”.

23 **SEC. 8. FEDERAL COMPUTER SYSTEM SECURITY TRAINING.**

24 Section 5(b) of the Computer Security Act of 1987
25 (40 U.S.C. 759 note) is amended—

1 (1) by striking “and” at the end of paragraph
2 (1);

3 (2) by striking the period at the end of para-
4 graph (2) and inserting in lieu thereof “; and”; and

5 (3) by adding at the end the following new
6 paragraph:

7 “(3) to include emphasis on protecting sensitive
8 information in Federal databases and Federal com-
9 puter sites that are accessible through public net-
10 works.”.

11 **SEC. 9. COMPUTER SECURITY FELLOWSHIP PROGRAM.**

12 There are authorized to be appropriated to the Sec-
13 retary of Commerce \$500,000 for fiscal year 2002 and
14 \$500,000 for fiscal year 2003 for the Director of the Na-
15 tional Institute of Standards and Technology for fellow-
16 ships, subject to the provisions of section 18 of the Na-
17 tional Institute of Standards and Technology Act (15
18 U.S.C. 278g–1), to support students at institutions of
19 higher learning in computer security. Amounts authorized
20 by this section shall not be subject to the percentage limi-
21 tation stated in such section 18.

1 **SEC. 10. STUDY OF ELECTRONIC AUTHENTICATION TECH-**
2 **NOLOGIES BY THE NATIONAL RESEARCH**
3 **COUNCIL.**

4 (a) REVIEW BY NATIONAL RESEARCH COUNCIL.—
5 Not later than 90 days after the date of the enactment
6 of this Act, the Secretary of Commerce shall enter into
7 a contract with the National Research Council of the Na-
8 tional Academy of Sciences to conduct a study of elec-
9 tronic authentication technologies for use by individuals,
10 businesses, and government.

11 (b) CONTENTS.—The study referred to in subsection
12 (a) shall—

13 (1) assess technology needed to support elec-
14 tronic authentication technologies;

15 (2) assess current public and private plans for
16 the deployment of electronic authentication tech-
17 nologies;

18 (3) assess interoperability, scalability, and in-
19 tegrity of private and public entities that are ele-
20 ments of electronic authentication technologies; and

21 (4) address such other matters as the National
22 Research Council considers relevant to the issues of
23 electronic authentication technologies.

24 (c) INTERAGENCY COOPERATION WITH STUDY.—All
25 agencies of the Federal Government shall cooperate fully
26 with the National Research Council in its activities in car-

1 rying out the study under this section, including access
2 by properly cleared individuals to classified information if
3 necessary.

4 (d) REPORT.—Not later than 18 months after the
5 date of the enactment of this Act, the Secretary of Com-
6 merce shall transmit to the Committee on Science of the
7 House of Representatives and the Committee on Com-
8 merce, Science, and Transportation of the Senate a report
9 setting forth the findings, conclusions, and recommenda-
10 tions of the National Research Council for public policy
11 related to electronic authentication technologies for use by
12 individuals, businesses, and government. The National Re-
13 search Council shall not recommend the implementation
14 or application of a specific electronic authentication tech-
15 nology or electronic authentication technical specification
16 for use by the Federal Government. Such report shall be
17 submitted in unclassified form.

18 (e) AUTHORIZATION OF APPROPRIATIONS.—There
19 are authorized to be appropriated to the Secretary of Com-
20 merce \$450,000 for fiscal year 2002, to remain available
21 until expended, for carrying out this section.

22 **SEC. 11. PROMOTION OF NATIONAL INFORMATION SECU-**
23 **RITY.**

24 The Under Secretary of Commerce for Technology
25 shall—

(1) promote an increased use of security techniques, such as risk assessment, and security tools, such as cryptography, to enhance the protection of the Nation's information infrastructure;

(2) establish a central repository of information for dissemination to the public to promote awareness of information security vulnerabilities and risks; and

(3) in a manner consistent with section 12(d) of the National Technology Transfer and Advancement Act of 1995 (15 U.S.C. 272 nt), promote the development of national standards-based infrastructures needed to support government, commercial, and private uses of encryption technologies for confidentiality and authentication.

SEC. 12. ELECTRONIC AUTHENTICATION INFRASTRUCTURES.

(a) ELECTRONIC AUTHENTICATION INFRASTRUCTURES.—

(1) TECHNOLOGY-NEUTRAL GUIDELINES AND STANDARDS.—Not later than 18 months after the date of the enactment of this Act, the Director, in consultation with industry and appropriate Federal agencies, shall develop technology-neutral guidelines and standards, or adopt existing technology-neutral industry guidelines and standards, for electronic au-

1 authentication infrastructures to be made available to
2 Federal agencies so that such agencies may effec-
3 tively select and utilize electronic authentication
4 technologies in a manner that is—

5 (A) adequately secure to meet the needs of
6 those agencies and their transaction partners;
7 and

8 (B) interoperable, to the maximum extent
9 possible.

10 (2) ELEMENTS.—The guidelines and standards
11 developed under paragraph (1) shall include—

12 (A) protection profiles for cryptographic
13 and noncryptographic methods of authen-
14 ticating identity for electronic authentication
15 products and services;

16 (B) a core set of interoperability specifica-
17 tions for the use of electronic authentication
18 products and services in electronic transactions
19 between Federal agencies and their transaction
20 partners; and

21 (C) validation criteria to enable Federal
22 agencies to select cryptographic electronic au-
23 thentication products and services appropriate
24 to their needs.

1 (3) REVISIONS.—The Director shall periodically
2 review the guidelines and standards developed under
3 paragraph (1) and revise them as appropriate.

4 (b) LISTING OF PRODUCTS.—Not later than 30
5 months after the date of the enactment of this Act, and
6 thereafter, the Director shall maintain and make available
7 to Federal agencies a nonmandatory list of commercially
8 available electronic authentication products, and other
9 such products used by Federal agencies, evaluated as con-
10 forming with the guidelines and standards developed
11 under subsection (a).

12 (c) SPECIFICATIONS FOR ELECTRONIC CERTIFI-
13 CATION AND MANAGEMENT TECHNOLOGIES.—

14 (1) SPECIFICATIONS.—The Director shall, as
15 appropriate, establish core specifications for par-
16 ticular electronic certification and management tech-
17 nologies, or their components, for use by Federal
18 agencies.

19 (2) EVALUATION.—The Director shall advise
20 Federal agencies on how to evaluate the conform-
21 ance with the specifications established under para-
22 graph (1) of electronic certification and management
23 technologies, developed for use by Federal agencies
24 or available for such use.

1 (3) MAINTENANCE OF LIST.—The Director
2 shall maintain and make available to Federal agen-
3 cies a list of electronic certification and management
4 technologies evaluated as conforming to the speci-
5 fications established under paragraph (1).

6 (d) REPORTS.—Not later than 18 months after the
7 date of the enactment of this Act, and annually thereafter,
8 the Director shall transmit to the Congress a report that
9 includes—

10 (1) a description and analysis of the utilization
11 by Federal agencies of electronic authentication
12 technologies; and

13 (2) a description and analysis regarding the
14 problems Federal agencies are having, and the
15 progress such agencies are making, in implementing
16 electronic authentication infrastructures.

17 (e) DEFINITIONS.—For purposes of this section—

18 (1) the term “electronic authentication” means
19 cryptographic or noncryptographic methods of au-
20 thenticating identity in an electronic communication;

21 (2) the term “electronic authentication infra-
22 structure” means the software, hardware, and per-
23 sonnel resources, and the procedures, required to ef-
24 fectively utilize electronic authentication tech-
25 nologies;

1 (3) the term “electronic certification and man-
2 agement technologies” means computer systems, in-
3 cluding associated personnel and procedures, that
4 enable individuals to apply electronic authentication
5 to electronic information; and

6 (4) the term “protection profile” means a list of
7 security functions and associated assurance levels
8 used to describe a product.

9 **SEC. 13. SOURCE OF AUTHORIZATIONS.**

10 There are authorized to be appropriated to the Sec-
11 retary of Commerce \$7,000,000 for fiscal year 2002 and
12 \$8,000,000 for fiscal year 2003, for the National Institute
13 of Standards and Technology to carry out activities au-
14 thorized by this Act for which funds are not otherwise spe-
15 cifically authorized to be appropriated by this Act.

○